REMARKS/ARGUMENTS

This amendment and response is intended to be a complete response to the Office action of July 14, 2004 and the case is believed to be in condition for allowance. Accordingly, reconsideration is respectfully requested.

In the Specification

Applicant has amended the Specification to more clearly describe the invention. The changes made merely clarify that which may readily be discerned from the specification, claims and drawings as originally filed. Accordingly, no new matter has been added.

Status of the Claims

Claims 1-8 were rejected in the Office Action. Claim 1 is cancelled herein. Claims 9 through 13 are added herein. Claims 2-8 are amended herein. Claims 2-13 are now pending in the application.

The Drawings

The drawings were objected under 37 CFR 1.83(a) as not showing every feature of the claimed invention. Applicants have added three new drawings to illustrate the features claimed in Claims 3, 4, and 6. The subject matter of these drawings may readily be discerned from the specification, claims, and drawings as originally filed. Accordingly, no new matter has been added.

The Title

The Examiner stated that the title was not descriptive. Applicants thank the Examiner for suggesting a new title. Applicants have amended the specification to reflect this title and respectfully request that the Examiner take any necessary actions to effect this change in the official record of the application.

The Claims

35 USC 112, second paragraph

Claim 1 was rejected under 35 USC 112, second paragraph. Claim 1 has been cancelled. Thus, the objection is now moot.

35 USC 103

Claims 1 through 8 were rejected under 35 U.S.C.103(a) as unpatentable over Schneier Applied Cryptography 2^{nd} Edition (hereinafter Schneier) in view of Kocher "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" (hereinafter Kocher). Claim 1 has been cancelled. However, Applicants traverse the rejection with respect to Claims 2-7 and the newly added claims.

Schneier appears to merely be cited for the proposition of cryptographic algorithms. Schneier does not teach or suggest "random transformation of at least one of the data elements by associating said at lest one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type random transformation of at least one of the data elements by associating said at lest one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type" and the Examiner has admitted as much (Office Action, paragraph 10).

The Examiner has relied on Kocher to provide the lacking teaching from Schneier. However, Kocher also fails to teach or suggest at least one element of the claimed invention.

Kocher refers to a blind signature scheme which can briefly be described as follows:

Blinding signature is a concept in cryptography that allows a client to have a provider compute a mathematical function $y = f(x)$, where the client provides an input x and retrieves the corresponding output y, but the provider would neither learn x nor y.

In a typical setting, a provider offers to compute a function $fx(m)$ using some private key x and some input m chosen by a client. A client can send an input m, have the provider compute the corresponding result $z = fx(m)$ and retrieve z from the provider afterwards. With a blinding technique, a client would send a transformed input m^* to the provider, and would retrieve the corresponding result z^* in return. From this result, the client could then derive the result $z = fx(m)$ that corresponds to the input m in which the client was interested in the first place. Some blinding techniques guarantee that the provider learns no information about the client's input m and corresponding output z.

For Diffie-Hellman private-keys operations, the result R is obtained from the input data y, the key x and a module number n, as follows: $R = y^x \bmod (n)$.

Kocher fails to disclose a method for protecting data elements from discovery by analysis of the microprocessor's electric power consumption because Kocher refers only to timing attacks (and not power attacks), which timing attacks measure time delays between data input times and data output times for several different input data.

In addition, Kocher fails to disclose the random transformation of at least one of the data elements by associating said at least one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type. The use of a signature scheme proposed by Kocher is different from the invention recited in Claim 9 (which replaces cancelled Claim 1). In a signature scheme, the input data is signed by a key to produce an unpredictable data. In our scheme, the input data is "transformed" by a data which in unknown (random data) to produce an unpredictable data. By definition, it makes no sense in a blinding signature scheme that the private key to sign the input data be generated randomly. Otherwise the generation of the corresponding public key required for the inverse transformation step would be impossible. In fact, in a public/private key scheme, it is essential that from one of the keys with the key pair, you cannot deduce the corresponding other key.

For these reasons, a person of ordinary skill in the art would not be motivated to modify Kocher to arrive at applicants' claimed invention. Furthermore, the combination of Schneier with Kocher would still lack the limitation the random transformation of at least one of the data elements by associating said at least one of the data elements with a random number generated by an unpredictable number generator, by means of a logical operator of the exclusive-OR type. Accordingly, Claim 9 is patentable over Schneier and Kocher taken singly or in combination.

New claim 10, similarly, recites limitations not taught or suggested by Schneier and Kocher, taken singly or in combination. Accordingly, Claim 10 should be allowed for the same reasons given in support of Claim 9.

The various dependent claims incorporate all the limitations of their respective base claims, provide further unique and non-obvious combinations, and are patentable for the reasons given in support of the independent claims and by virtue of such further combinations.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request reconsideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Respectfully submitted,

Pehr B. Jansson
Registration No. 35,759

Date: December 14, 2004.

Customer No. 41754
Pehr Jansson
Pehr Jansson's Law Firm
7628 Parkview Circle
Austin, TX 78731
512-241-0837
Fax: 678-868-0101